Remarks

Claims 1-149 are currently pending in the present application. Claims 1, 95, and 129-148 have been amended. The Examiner is thanked for indicating that Claims 7, 9-39, 48-54, 69-94, 98-128, 131-147, and 149 include allowable subject matter. The Applicants submit that no new matter has been introduced herein. In view of the foregoing claim amendments and following remarks, reconsideration and withdrawal of the various grounds of rejection are respectfully requested.

Claim Rejections under 35 U.S.C. §112

Claims 129 – 147 stand rejected under 35 U.S.C. §112 as being indefinite. Claims 129-147 have been amended in accordance with the Examiner's helpful suggestions. In view of the foregoing amendments to Claims 129-147, the Applicants respectfully request reconsideration and withdrawal of this grounds of rejection.

Claim Rejections under 35 U.S.C. §102

Claims 1-5, and 8 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,848,158 to Saito et al., hereinafter "Saito". For the reasons set forth below, reconsideration and withdrawal of this grounds of rejection is respectfully requested.

Claim 1, as amended, is directed to a method for maintaining data security by providing a means for securely delivering data, and for regulating use of the data once it arrives at its desired destination. Data, together with one or more permissions for regulating use of the data, are bundled together thereby creating a bundled data package. The bundled data package is delivered to a receiver, wherein the bundled data package is processed. Upon processing the package, the data from the bundled package is stored in a vault. As used herein, a 'vault' refers to a space on a hard drive dedicated for storing secured data. Unlike other hard drive spaces, however, a vault is unique in that its existence, and the existence of any data stored therein, is invisible to a user of the receiver. (see page 4, line 21 to page 6, line 12 of the specification).

Saito, to the contrary, is directed to a system for managing, and subsequently charging users for the use of copyrighted data. According to Saito, copyrighted data is first scrambled or encrypted and then provided to a user. (see column 4, lines 26-30 and lines 37-40 of Saito). If the user desires to view, copy, store, edit, and or otherwise use the scrambled data, the user is required to request a primary use permit key (K1) by presenting a primary label (Lc1) to a key control center (12) via a network system (14). (see Figure 2 system and column 5, lines 32-37 of Saito). Upon receiving the

request from the user, the key control center (12) searches for the requested primary use permit key (K1) using the primary label (Lc1) provided by the user. (see column 5, lines 38-43 of Saito). If the permit key (K1) is located, the key control center (12) transmits the permit key (K1) to the user over a network system, and at the same time, charges the user a predetermined fee for use of the copyrighted data. (Id.). The user utilizes the key (K1) to decrypt the data and utilizes the data according to the content of the *use permit key (K1)*. (emphasis added). (see column 5, lines 43-50, and column 6, lines 62-65 of Saito). If the user wishes to utilize the data in a manner not specified by the primary permit key (K1), the user is required to request a secondary key, for example, an edit key, in order to so utilize the data. (see column 5, lines 60-64 of Saito).

Unlike Claim 1, Saito fails to recite bundling data *and* one or more permissions into a package and then providing the packaged bundle to a user. Instead, Saito discloses first providing encrypted data to a user. Then, and only in response to a request by the user, Saito discloses providing a primary use permit key (K1) to the user for use in decrypting the encrypted data. (see column 5, lines 32-37 of Saito). As noted above, "...utilization of the copyrighted data is restricted according to the content of the use permit key." (see column 6, lines 61-65 of Saito). Thus, any permissions associated with regulating use of the data are provided as content in a use permit key. Since Saito fails to disclose bundling the data with one or more use permit keys, Saito fails to disclose bundling data with one or more permissions, as recited in Claim 1.

Furthermore, Saito fails to disclose storing the data in a vault. As noted above, a vault refers to allocated space on a receiver's hard drive for protecting and hiding vault contents. The location and/or contents of the vault remain invisible to a user. With regard to storage, Saito merely discloses re-encrypting data before storing it, "...[the data] is re-encrypted using a first crypt key K1*i*...and the re-encrypted copyrighted primary data ED1*i* is stored." (see column 5, lines 50-57 of Saito). Saito makes no mention of a vault, or even of allocating secure space on a hard drive (which remains hidden to a user) for storing copyrighted data. Thus, the user in Saito is not precluded from locating and/or copying the copyrighted data (say, onto a clipboard) for transfer to another system.

Since Saito fails to disclose both a bundled package comprising data and permissions, and storing data in a vault, the Applicants submit that Saito fails to disclose each and every claim feature recited in Claim 1.

The Office Action, however, cites column 2, lines 60-67 of Saito as disclosing these features.

A close examination of Saito, however, reveals otherwise. The cited section of Saito discloses that a copyright management program "...watches and manages in such manner that no utilization of data is performed beyond the conditions of request or permission." (see column 2, lines 59-61 of Saito). Saito goes on to explain that data is encrypted and supplied to a user, and is then decrypted using a use permit key. (see column 2, lines 62-63 of Saito). This management program, however, does not provide permissions. As discussed above, permissions are provided in permit keys, "...a permit key is provided for each utilization such as displaying, using, storing, copying, editing, transferring, etc." (see column 2, lines 63-67 of Saito). Therefore, since Saito fails disclose bundling one or more permissions with data, Saito fails to disclose each and every claim feature of Claim 1. Accordingly, the Applicants submit that Claim 1 is not anticipated by Saito and respectfully request reconsideration and withdrawal of this grounds of rejection.

Claim 2 depends from Claim 1, and recites an opening the package (comprising data and one or more permissions) and verifying the receiver for processing the package. As explained above, Saito fails to disclose a package having data bundled together with one or more permissions. Saito also fails to disclose verifying the receiver. The Office Action looks to column 5, lines 24-45 of Saito for disclosing these features, however, a close examination of Saito reveals otherwise. According to the cited portion of Saito, encrypted data is supplied to a user; the user requests a use permit key K1 by presenting a copyright label Lc1; a key control center 12 searches for the use permit key K1 using the copyright label Lc1 provided by the user, and transmits the permit key K1 to the user via a network; and upon receiving the permit key K1, the user decrypts and uses the data. (see column 5, lines 24-45 of Saito). Saito makes no mention of opening a package, nor of verifying a receiver. Any presenter of the copyright label Lc1 will be provided with a use permit key K1, without regard to the requesting receiver. Thus, for at least these reasons, the Applicants submit that Saito fails to disclose each and every claim feature of Claim 2. Accordingly, reconsideration and withdrawal of this grounds of rejection is respectfully requested.

Claim 3 indirectly depends from Claim 1, and recites searching for at least one driver for reading the package. As discussed above, Saito fails to disclose a package comprising data bundled together with one or more permissions. Furthermore, Saito fails to disclose searching for a driver. The Office Action looks to column 2, lines 45-55 ("Program to manage copyright", and column 4, lines 50-60 of Saito as disclosing these features). An examination of Saito, however, reveals

otherwise. According to Saito, one or more programs for managing copyrighted information are transmitted, when needed, along with a use permit key to allow a user to utilized encrypted data. (see column 2, lines 45-55 of Saito); and a key control center is utilized for controlling use permit keys (column 4, 50-60 of Saito). In sum, Saito discloses providing a use permit key for use in decrypting copyrighted data. Saito does not disclose, however, *searching* for a driver in the receiver that is capable of reading a bundled package comprising data plus one or more permissions. In fact, Saito does not even disclose a driver at all. Thus, for at least these reasons, the Applicants submit that Claim 3 is not anticipated by Saito and respectfully request reconsideration and withdrawal of this grounds of rejection.

Claim 4 depends from Claim 1, and recites detecting violation of one or more permissions. As discussed above, Saito fails to disclose a package having data bundled together with one or more permissions. Thus, for at least those reasons discussed above with regard to Claim 1, the Applicants submit that Claim 4 is not anticipated by Saito and respectfully request reconsideration and withdrawal of this grounds of rejection.

Claim 5 indirectly depends from Claim 1, and recites providing internal security. Internal security, as used in Claim 5, refers to additional security features contained *within the vault* for use in further preventing unauthorized access to protected data stored in the vault, as opposed to providing general security internal to a receiver. (see page 5, lines 17-26 of the specification). As discussed above, Saito fails to disclose a vault. Furthermore, Saito fails to disclose providing security within the vault for further protecting data. The Office Action looks to column 4, lines 50-59 of Saito for disclosing this feature, however, a close examination of Saito reveals otherwise. According to the cited portion of Saito, a personal computer having an operating system (OS) includes security processing incorporated therein, and storage space for storing a copyright management program and crypt keys. (see column 4, lines 50-59 of Saito). Saito neither discloses a vault, nor does it disclose providing security features within the vault, as recited in Claim 5. At most, Saito discloses hard disk space and security processing generally within a personal computer. Providing general security within a personal computer and storing a management program and crypt keys on hard disk space is not equivalent to providing hidden space on a hard drive for storing data, wherein the hidden space has additional security features built therein. Thus, for at least these reasons, the Applicants submit that Saito fails to disclose each and every claim feature of Claim 5. Accordingly, reconsideration and

withdrawal of this grounds of rejection is respectfully requested.

Claim 8 depends from Claim 5, and recites a package further comprising an executable program which verifies that a receiver is operating, i.e., that the receiver is running. (see page 4, lines 30-32 of the specification). As discussed above, Saito fails to disclose a package having data bundled together with one or more permissions. Saito also fails to disclose providing an executable program for *verifying that the receiver is running*. (emphasis added). The Office Action looks to column 5, lines 24-45 of Saito for disclosing these features. According to the cited portion of Saito, encrypted data is supplied to a user; the user requests a use permit key K1 by presenting a copyright label Lc1; a key control center 12 searches for the use permit key K1 using the copyright label Lc1 provided by the user, and transmits the permit key K1 to the user via a network; and upon receiving the permit key K1, the user decrypts and uses the data. (see column 5, lines 24-45 of Saito). Saito does not mention an executable program *within a package* which determines whether the receiver is running. (emphasis added). In fact, as discussed above with respect to Claim 2, Saito fails to disclose any form of verification whatsoever. Thus, for at least these reasons, the Applicants submit that Saito fails to disclose each and every claim feature of Claim 8. Accordingly, reconsideration and withdrawal of this grounds of rejection is respectfully requested.

Claims 95-97, 129, 130, and 148 stand rejected under 35 U.S.C. §102(e) as being anticipated by U. S. Patent No. 5,933,498 to Schneck et al., hereinafter "Schneck". For the reasons set forth below, reconsideration and withdrawal of this grounds of rejection is respectfully requested.

Claims 95 and 129, as amended, recite a package comprising data bundled together with one or more permissions and storing data within a vault for restricted access to the data. As discussed above with regard to Claim 1, a 'vault' as used herein describes a space on the hard drive dedicated for storing secured data. Unlike other hard drive spaces, however, a vault is unique in that its existence, and the existence of any data stored therein, is invisible to a user of the receiver. (see page 4, line 21 to page 6, line 12 of the specification).

Schneck, on the other hand, is directed to a system for protecting portions of data by determining rules concerning access to the data, transmitting the data and access rules to a user, and enabling the user, via an access mechanism, to access the data according to the access rules. (see Abstract of Schneck). Schneck fails to disclose, however, storing the data in a vault. The Office Action looks to Figure 1, and column 15 line 50 to column 16, line 20 of Schneck as disclosing this

feature. According to Schneck, an access mechanism 114 comprises a plurality of components which are packaged in such a way as to detect tampering with the mechanism 114 and to disable the mechanism 114 upon such detection. (see column 15, line 50 to column 16, line 20 of Schneck). Forms that this access mechanism 114 may take include a laptop computer, which "...meets all the requirements of having all components within the same physical package or case" (see column 16, lines 23-25 of Schneck); or an external co-processor of another computer or processor which gets plugged-in to the computer or processor 170 (see Figure 9 and column 16, lines 27-38 of Schneck).

The access mechanism 114 is not the functional equivalent of a vault, as recited in Claims 95 and 129. The vault of Claims 95 and 129 refers to invisible space on a hard drive which is undetectable by a user. Since the user can not detect the presence of the vault, it is virtually impossible for the user to tamper with the vault. The access mechanism 114 of Schneck, however, is readily visible and accessible by the user, hence the need for tamper detection. In addition, the access mechanism 114 of Schneck requires a plurality of components physically packaged together in a single case (as in a lap-top computer); or alternatively, the access mechanism may be an external processor for use with a computer. In either event, the access mechanism 114 does not refer to invisible space on a hard drive which is internal to a receiver, as recited in Claims 95 and 129. Thus, for at least these reasons, the Applicants submit that Schneck fails to disclose each and every claim feature of Claims 95 and 129, and respectfully request reconsideration and withdrawal of the 35 U.S.C. §102 grounds of rejection.

Claim 96 depends from Claim 95, and recites providing internal security. Internal security, as used in Claim 96, refers to additional security features contained *within the vault* for use in further preventing unauthorized access to protected data stored in the vault, as opposed to providing general security internal to a receiver. (see page 5, lines 17-26 of the specification). As discussed above, Schneck fails to disclose a vault. Thus, Schneck fails to disclose providing security within the vault for further protecting data. The Office Action again looks to column 15, line 50 to column 16 line 20 of Schneck for disclosing this feature, however, a close examination of Schneck reveals otherwise. As discussed in detail with regard to Claim 95 above, Schneck recites an access mechanism 114 which refers to a bundle of components encased in a single package (e.g., a lap-top computer), or an external processor which is plugged into a main computer. (see column 15, line 50 to column 16, line 20 of Schneck). Since Schneck fails to disclose a vault, i.e., hidden space on a hard drive which

is invisible to a user, Schneck also fails to disclose providing internal security which is internal to the vault, as recited in Claim 96. Thus, for at least these reasons, the Applicants submit that Schneck fails to disclose each and every claim feature of Claim 96. Accordingly, reconsideration and withdrawal of this grounds of rejection is respectfully requested.

Claims 97 and 130 indirectly depend from Claims 95 and 129, respectively, and disclose detecting violation of one or more permissions. As discussed above, Schneck fails to disclose the main features of independent Claims 95 and 129, from which Claims 97 and 130 depend, respectively. Thus, for at least those reasons discussed above with regard to Claims 95 and 129, the Applicants submit that Claims 97 and 130 are not anticipated by Schneck and respectfully request reconsideration and withdrawal of this grounds of rejection.

Claim 148 as amended recites a system comprising a first computer for creating a package bundled together with data, and a second computer for receiving the package, opening the package, and storing the data within a vault. As discussed above with regard to Claims 95 and 129, Schneck fails to disclose storing restricted data within a vault located within a receiver, in this case, the second computer. The additional sections of Schneck cited by the Office Action (i.e., column 18, lines 10-60 and Figures 1-3 of Schneck) do nothing to cure this deficiency. Column 18, lines 10-60 of Schneck merely discloses a method implemented by the access mechanism 114 for restricting access to a user. A vault for storing the data, however, is not disclosed. Thus, for at least these reasons, the Applicants submit that Schneck fails to disclose each and every claim feature of Claim 148. Accordingly, reconsideration and withdrawal of this grounds of rejection is respectfully requested.

Claim Rejections under 35 U.S.C. §103

Claims 6, 40-47, and 55-65 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Saito in view of U. S. Patent No. 5,283, 828 to Saunders et al., hereinafter "Saunders". For the reasons set forth below, reconsideration and withdrawal of this grounds of rejection is respectfully requested.

Claim 6 depends from Claim 5, and recites creating a tag file corresponding to the data, mapping the tag file to a virtual table, and storing the virtual table in the vault. As discussed above with regard to Claim 5, Saito fails to disclose a package having data bundled together with one or more permissions, and a vault for storing data. Since Saunders does nothing to cure the deficiencies

of Saito, a Saito-Saunders combination fails to disclose each and every feature of Claim 6.

As noted by the Office Action, Saito fails to disclose creating a tag file, mapping it to a virtual table, and storing the data and virtual table in the vault. The Office Action looks to Saunders for providing these features. A close examination of Saunders, however, reveals otherwise. Saunders is directed to an architecture adapted for use on a base computer for utilizing co-processing systems to increase security. (see Abstract of Saunders). Saunders does not disclose packaging data with one or more permissions, nor does it disclose a vault. Instead, Saunders discloses uniquely identifying objects by storing object identifiers in a global object table (GOT).(see column 6, lines 49-59 of Saunders). The GOT and data objects, however, are on suitable media, as opposed to in a vault. (emphasis added). (Id). Thus, since Saunders does not disclose storing its GOT and system objects in a vault, which as previously discussed, refers to invisible space on a hard drive; and since Saunders fails to cure the deficiencies of Saito (i.e., by failing to disclose a package and a vault), the Applicants submit that a Saito-Saunders combination fails to disclose each and every feature of Claim 6. Thus, for at least these reasons, reconsideration and withdrawal of the obviousness grounds of rejection is respectfully requested.

Claims 40-44 depend from Claim 5, and indirectly from Claim 1, and recite providing data security in a first device driver operably installed in a computer operating system having a layered plurality of device drivers for accessing data. As duly noted by the Office Action, the method of Claims 40-44 is not disclosed by a Saunders-Saito combination. However, the Office Action relies on Official Notice that such a process is known, and that the additional features of Claims 40-44 are obvious in view of a Saunders-Saito combination. The Office Action, however, has not provided factual support for such Official Notice. Accordingly, the Applicants respectfully request that the PTO provide an Affidavit of Official Notice, in accordance with 37 C.F.R. 1.104(d)(2), with respect to the process of Claims 40-44.

As discussed above, neither Saito, Saunders, nor a combination thereof disclose the main features of Claims 5 and 1, from which Claims 40-44 depend. Namely, a Saunders-Saito combination fails to disclose bundling data and one or more permissions into a package, opening the package and storing the data in a vault within the receiver, and providing additional security features within the vault for protecting the restricted data. Furthermore, neither Saunders nor Saito discloses a device driver operably installed in a computer operating system having a layered plurality of device

derivers. With regard to the Office Actions official notice, the Official Notice fails to disclose determining whether the first driver is functionally uppermost in the layered plurality of layers, and performing I/O requests according to said determination.

Therefore, for at least these reasons, the Applicants respectfully submit that a combination of Saunders-Saito-and the Office Action's Official Notice fails to disclose each and every feature of Claims 40-44. Accordingly, the Applicants request reconsideration and withdrawal of this grounds of rejection.

Claim 45 depends from Claim 40, and recites a method for determining whether a driver is functionally uppermost in the layered plurality of device drivers. As discussed above with regard to Claim 40, a combination of Saunders-Saito-and Official Notice fails to disclose each and every feature of Claim 40, from which Claim 45 depends. Thus, for at least those reasons, Claim 45 is not obvious. Accordingly, the Applicants request reconsideration and withdrawal of this grounds of rejection.

As duly noted by the Office Action, the method of Claim 45 is not disclosed by a Saunders-Saito combination. The Office Action relies on Official Notice that such a process is known, and that the additional features of Claim 45 are obvious in view of a Saunders-Saito combination. The Office Action, however, has not provided adequate factual support for such Official Notice. Accordingly, the Applicants respectfully request that the PTO provide an Affidavit of Official Notice, in accordance with 37 C.F.R. 1.104(d)(2), with respect to the process of Claim 45.

Claims 46 and 47 depend from Claim 40, and recite denying an I/O request in the secure first device driver. As duly noted by the Office Action, the method of Claims 46 and 47 are not disclosed by a Saunders-Saito combination. However, the Office Action relies on Official Notice that such a process is known, and that the additional features of Claims 46 and 47 are obvious in view of a Saunders-Saito combination. The Office Action, however, has not provided adequate factual support for such Official Notice. Accordingly, the Applicants respectfully request that the PTO provide an Affidavit of Official Notice, in accordance with 37 C.F.R. 1.104(d)(2), with respect to the process of Claims 46 and 47.

As discussed above, neither Saito, Saunders, nor a combination thereof disclose the main features of Claim 40, from which Claims 46 and 47 depend. Therefore, for at least these reasons, the Applicants respectfully submit that a combination of Saunders-Saito-and the Office Action's Official

Notice fails to disclose each and every feature of Claims 46 and 47. Accordingly, the Applicants request reconsideration and withdrawal of this grounds of rejection.

Claims 55-57 depend from Claim 1, and recite security steps in authorizing port access requests. As duly noted by the Office Action, the method of Claims 55-57 is not disclosed by a Saunders-Saito combination. However, the Office Action relies on Official Notice that such a process is known, and that the additional features of Claims 55-57 are obvious in view of a Saunders-Saito combination. As discussed above, neither Saito, Saunders, nor a combination thereof disclose the main features of Claim 1, from which Claims 55-57 depend. Namely, a Saunders-Saito combination fails to disclose bundling data and one or more permissions into a package, and storing the data in a vault within the receiver. Therefore, for at least these reasons, the Applicants respectfully submit that a combination of Saunders-Saito-and the Office Action's Official Notice fails to disclose each and every feature of Claims 55-57. Accordingly, the Applicants request reconsideration and withdrawal of this grounds of rejection.

Claims 58-62 depend from Claim 5, and indirectly from Claim 1, and recite a method for providing internal security. As duly noted by the Office Action, the method of Claims 58-62 is not disclosed by a Saunders-Saito combination. However, the Office Action relies on Official Notice that such a process is known, and that the additional features of Claims 58-62 are obvious in view of a Saunders-Saito combination. The Office Action, however, has not provided adequate factual support for such Official Notice. Accordingly, the Applicants respectfully request that the PTO provide an Affidavit of Official Notice, in accordance with 37 C.F.R. 1.104(d)(2), with respect to the method of Claims 58-62.

As discussed above, neither Saito, Saunders, nor a combination thereof disclose the main features of Claims 5 and 1, from which Claims 58-62 depend. Namely, a Saunders-Saito combination fails to disclose bundling data and one or more permissions into a package, opening the package and storing the data in a vault within the receiver, and providing additional security features within the vault for protecting the restricted data. Therefore, for at least these reasons, the Applicants respectfully submit that a combination of Saunders-Saito-and the Office Action's Official Notice fails to disclose each and every feature of Claims 58-62. Accordingly, the Applicants request reconsideration and withdrawal of this grounds of rejection.

Claims 63-65 depend from Claim 5, and indirectly from Claim 1, and recite a method for

providing internal security. As duly noted by the Office Action, the method of Claims 63-65 is not disclosed by a Saunders-Saito combination. However, the Office Action relies on Official Notice that such a process is known, and that the additional features of Claims 63-65 are obvious in view of a Saunders-Saito combination. As discussed above, neither Saito, Saunders, nor a combination thereof disclose the main features of Claims 5 and 1, from which Claims 63-65 depend. Therefore, for at least these reasons, the Applicants respectfully submit that a combination of Saunders-Saito-and the Office Action's Official Notice fails to disclose each and every feature of Claims 63-65. Accordingly, the Applicants request reconsideration and withdrawal of this grounds of rejection.

Claims 66-68 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Saito in view of Schneck. For the reasons set forth below, reconsideration and withdrawal of this grounds of rejection is respectfully requested.

Claim 66 depends from Claim 1, and recites encrypting the data package and generating a computer executable file comprising the encrypted package. As discussed above with regard to Claim 1, Saito fails to disclose data bundled together with one or more permissions. As discussed with regard to Claims 95 and 129, Schneck fails to disclose storing the data in a vault. Instead, Schneck discloses an access mechanism 114 comprising a plurality of components which are packaged for storing data. This access mechanism 114 may be, for example, a plurality of devices packaged together (e.g., laptop computer), or an external co-processor of another computer or processor 170 which gets plugged-in to the computer or processor 170 (see Figure 9 and column 16, lines 27-38 of Schneck). Therefore, since both Saito and Schneck fails to disclose the main features of Claim 1, from which Claim 66 depends, the Applicants submit that a Saito-Schneck combination fails to disclose each and every feature of Claim 66. Accordingly, the Applicants request reconsideration and withdrawal of this grounds of rejection.

Claim 67 indirectly depends from Claim 1, and recites one or permissions selected from a recited group. As discussed above with regard to Claim 66, Saito fails to disclose data bundled together with one or more permissions, and Schneck fails to disclose a vault. Therefore, for at least those reasons discussed above with regard to Claim 66, the Applicants submit that a Saito-Schneck combination fails to disclose each and every feature of Claim 67. Furthermore, the Office Action looks to Figure 3 of Schneck for providing the additional features of Claim 67. A close examination of Figure 3, however, reveals otherwise. Figure 3 of Schneck does not disclose an access time

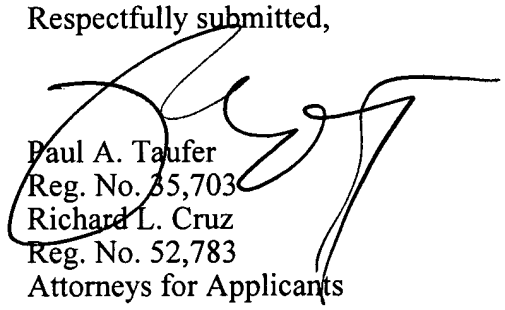
permission, an expiration date permission, an authorization data permission, a clipboard permission, a print permission, an unlimited access permission, an application permission, nor a system-events permission. Accordingly, since a Saito-Schneck combination fails to disclose each and every feature of Claim 67, the Applicants request reconsideration and withdrawal of the obviousness grounds of rejection.

Claim 68 depends from Claim 67, and recites setting a password for access to the computer executable file. As duly noted by the Office Action, a Saito-Schneck combination fails to disclose the method according to Claim 67, further comprising setting a password for the executable program. The Office Action, however, relies on Official Notice for providing this claim feature. As discussed above, however, a Saito-Schenck combination fails to disclose the claim features of Claims 1, 66, and 67, from which Claim 68 depends. Therefore, for at least those reasons discussed above with regard to Claims 1, 66, and 67, the Applicants submit that a Saito-Schneck-and Official Notice combination fails to disclose each and every feature of Claim 68. Therefore, the Applicants request reconsideration and withdrawal of the obviousness grounds of rejection.

Conclusion

In view of the foregoing amendments and remarks, the Applicants respectfully submit that the present Application, including Claims 1-149, is now in condition for allowance and respectfully request respectfully an indication reflecting the same.

Respectfully submitted,



Paul A. Taufer
Reg. No. 35,703
Richard L. Cruz
Reg. No. 52,783
Attorneys for Applicants

PAT/RLC/nn
(215) 656-3385